CHAPTER:1: POSSIBLE ATTACKS ON COMPUTER

1.1 THE NEED FOR SECURITY

Network Security

⇒ Network Security protects your network and data from breaches, intrusions and other threats.

⇒ Network Security involves access control, virus and antivirus software, application security, network analytics, firewalls and more.

Need of Security

⇒ The growing computer implies a need for automated tools for protecting files and other information.

⇒ In computer network, the need for security is must all communication from sender to receiver can be possible in a secure manner.

⇒ Security aspects in a computer network provide, privacy, authentication and integrity.

⇒ As there is a chance of attack by the third party while the sender making communication with receiver.

⇒ The security is needed for the following given reasons:

i) To protect the secret information users on the net only. No other person should access or see it.

ii) To protect the information from unwanted editing, accidently or intentionally by unauthorized users.

iii) To protect the information from loss and make it to be delivered to its destination properly.

iv) To manage for acknowledgement of message received by any node in order to protect from denial by sender situations. For example let a customer orders to purchase a few shares XYZ to the broader and denies for the order after two days as the rates go download.

ScannedbyCamScanner

v) To restrict a user to send some message to another with name of a third one.

vi) To protect the message from unwanted delay in the transmission lines/route in order to deliver it to required destination in time, incase of urgency.

Modern Nature of Attacks

The salient features of the modern nature of attack are as follows:

1) Automating Attacks:

- Automating attack can cause destruction by producing repetetive task. For example, they would excel in somehow stealing a very low amount (say half a dollar or 20 ruppees) from a million bank accounts in a matter of a few minutes. This would give the attacker a half million dollars possibly without any major complaints!

ii) Privacy Concern:

It means collecting information about people and later misusing it to create a huge problem so that privacy concerns of the people are loss due to attack.

iii) Distance does not matter:

Now-a-days the attack know it to move from one place to another place to still some vital information about a user. The attacker by sitting at its home can steal all the information about the user.

1.2. SECURITY APPROACH

1) Trusted Systems:

→ A trusted system is a computer system that can be trusted to a specified extent to enforce a specified security policy.

→ Trusted systems often use the term reference monitor i.e., an act entity responsible for all decision related to access controls

ScannedbyCamScanner

→ A reference monitor should be —

* Tamper-proof
* Invoked Always
* Small enough so that it can be tested independently

→ TCB (Trusted Computing Base) was defined as a combination of hardware, software and firmware responsible for enforcing the system's security policy.

2) Security Models:

An organisation can take several approaches to implement its security model. and these approaches are:

I) No Security →

In this approach, it could be a decision to implement no security at all.

II) Security Through Obscurity →

In this model, a system is secure simply because nobody knows about its exitence and contents. This approach cannot work for too long, as there are many ways an attacker can come to know about it.

III) Host Security →

In this model, the security for each host is enforced individually. This is a very safe approach, but the trouble is that it cannot scale well. The complexity and diversity of modern sites/organisations make the task even harder. Host security is tough to achieve as organisation grows and become more diverse.

IV) Network Security →

In this model, the focus is to control network access to various hosts and their services, rather than individual host security. This is a very efficient and scalable model.

Prepared by
Biswa Bandita Mohanty

ScannedbyCamScanner

3) Security Management Pratices

⇒ Good security management pratices always talk of security policy being in place,

⇒ Putting a security policy in place is actually quite and tough.

⇒ A good security policy generally takes care of four key aspects.

(I) Affordability

Cost and Effort in security implementation,

(II) Functionability

Mechanism of providing security

(III) Cultural Issues

Whether the policy gets well, with peoples expectations, working style and believes,

(IV) Legality

Whether the policy meets the legal requirement.

1.3. PRINCIPLES OF SECURITY

Once a security policy is in place, it should ensure -

a) Explanation of the policy to all concerned
b) Outline everybody's responsibilities
c) Use simple language in all communications.
d) Accountability should be established
e) Provide for exceptions and periodic receiver

Principles of Security

→ Principles of Security helps in understanding the attacks better and thinking of possible solutions to tackle them,

→ These are the four their principles of security. There are two more; access control and availability which are not related to a particular message, but are linked to the overall system as a whole.

Prepared by
Biswa Bandita Mohanty

ScannedbyCamScanner

① Confidentiality:

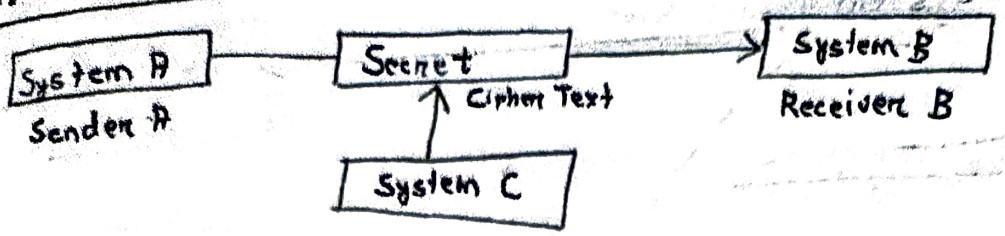


Fig. Loss of Confidentiality

→ Principle of Confidentiality specifies that only the sender and the intended receipient should be able to access the contents of a message.

→ Confidentiality gets compromised if an unauthorized person is access to a message.

→ A is meant to send a message to B but another user C gets access to this message which defeats the purpose of confidentiality.

→ The transfer of message from first user to the second user, which is accessed by third user without the permission or knowledge of A and B. This type of attact is called 'Interception'. (Causes loss of message confidentiality)

② Integrity:

→ When the contents of a message are changed or tampered after the sender sends it, but before it reaches the intended recipient, it is called that the integrity of the message is lost.

→ The contents of a message are changed or tampered by the third user without the knowledge of first user A (Sender) and second user B (receiver). The type of attack is called 'Modification'. (Causes loss of message integrity).

Prepared by
Biswa Bandita Mohanty

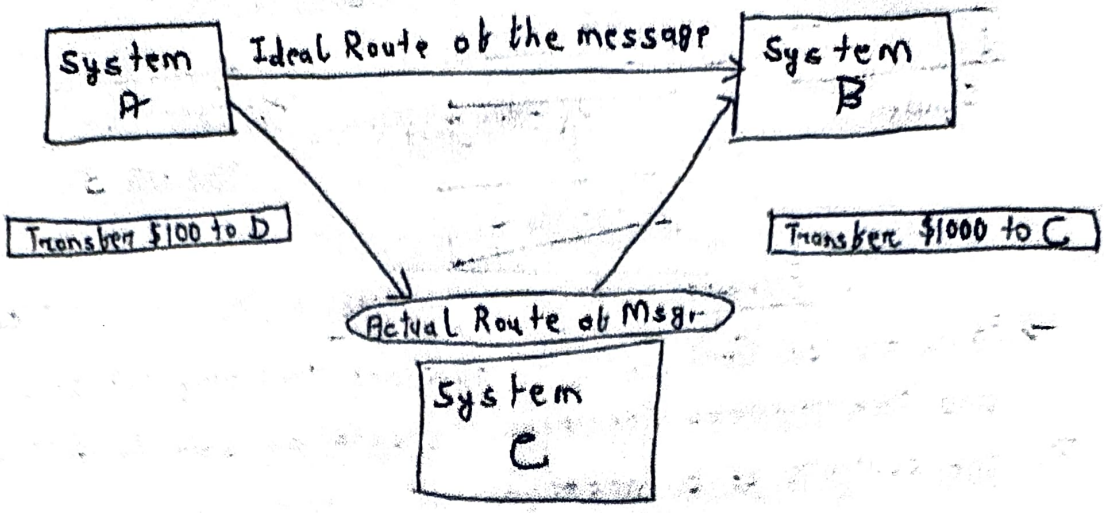


Fig. Loss of Integrity

③ Authentication:

→ Authentication mechanisms helps establishing proof of identities.

→ The authentication process ensures that the origin of an electronic message or document is correctly identified.

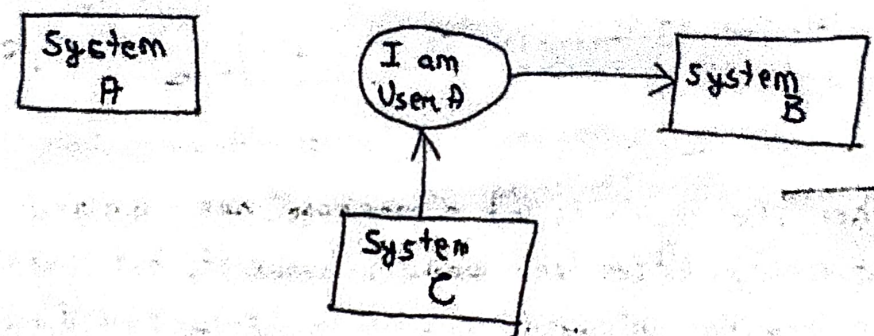


Fig. Absence of Authentication

Eg. System/user C sends an electronic document over Internet to user B. The trouble is user C had posed as user A. When he/she sent this document to user B, How would user B know that the message has come from user C, who is posing as user A. This type of attack is called 'fabrication'. (It is possible in absence of proper authentication mechanisms.)

(9) Non-repudiation:

→ Principle of Non-repudiation states that a user sends a message and later on refuses that he/she had sent that message.

→ The principle of non-repudiation defeats such possibility of denying something after having done it.

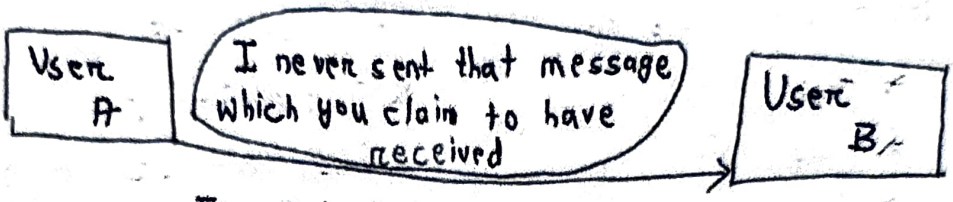


Fig. Establishing non-repudiation

→ Non-repudiation doesn't allow the sender of a message to refute the claim of not sending that message.

* Access Control:

→ The principle of access control determines who should be able to access what.

→ Access Control is broadly related to two areas - role management and rule management.

→ Role management concentrates on the user side, whereas rule management focuses on the resources side.

→ An Access Control List (ACL) is a subset of an access-control matrix.

→ Access control specifies and controls who can access what.

*Availability:

→ The principle of availability states that resources should be available to authorized parties at all times.

→ Interruption / Attack puts the availability of resources in danger.

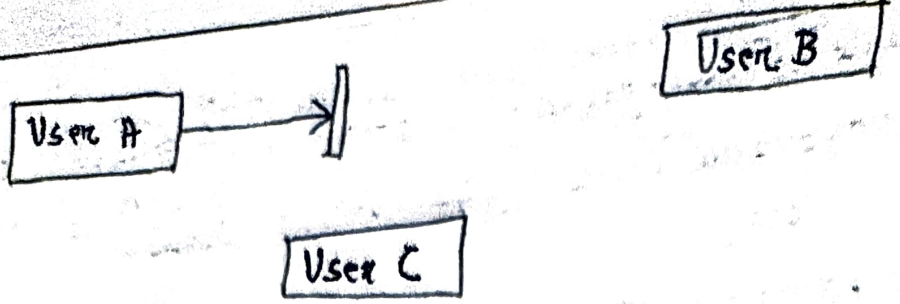


Fig. Attack on Availability

→ OSI standard for security model 7498-2 defines seven layers of security in the form of

* Authentication
* Access Control
* Non-repudiation
* Data Integrity.
* Confidentiality
* Assurance or Availability.
* Notarization or Signature

* Ethical and Legal Issues:

① Privacy → This deals with the right of an individual to control personal or sensitive information.

② Accuracy → This talks about the responsibility for the authenticity, fidelity and accuracy of information.

③ Property → The owner of information who controls access.

④ Accessibility → Deals with the issues of what information does an oraganisation have the right to collect;

e.g. Regulatory Bodies

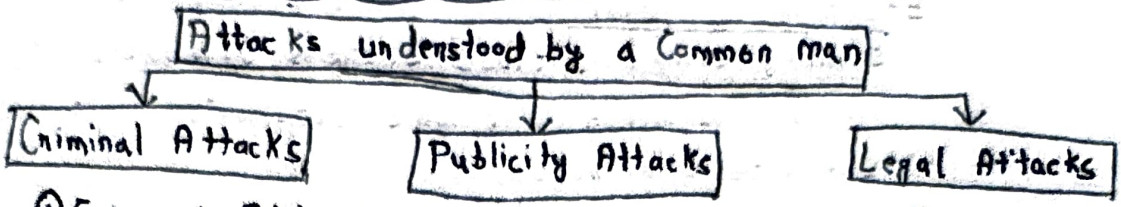
- International - International Cybercrime Treaty
- Federal - FERPA, GLB, DMCA, HIPAA, Teach Act, etc.
- State - UCITA, SB 1386, etc.
- Organization - Computer use policy

Prepared by
Biswa Bandita Mohanty

1.4 TYPES OF ATTACKS

→ Attacks – Attacks are unauthorized actions against private, corporate or governmental IT assets in order to destroy them, modify them or steal sensitive data.

1) General View of Attacks :



① Criminal Attacks → Criminal Attacks are the simplest to understand. The main aim of attackers is to maximize financial gain by attacking computer system.

Types of Criminal Attacks :

A- Fraud – Modern fraud attacks concentrate on manipulating some aspects of electronic ~~company~~ currency, credit cards, electronic stocks certificates, cheques, letters of credit, purchase orders, ATM, etc.

B- Scams – Sales of services, auctions, multilevel marketing schemes, general merchandise and business opportunities etc are some forms of scams. People are enticed to send money in return of great returns but endup losing their money. It happens in multiple users.

C- Destruction – Some sort of grudge is the motive behind such attacks.

Eg. In the year 2000, an attack against popular Internet sites such as Yahoo!, CNN, eBay, Buy.com, Amazon.com, where authorized users of these sites failed to log in or access these sites.

D- Identity Theft – An attacker doesn't steal anything from a legitimate user – he/she becomes that legitimate user.

Eg: Much easier to get password of someone else's bank a/c or getting credit card on someone else's name. Priviledge is misused until it gets detected.

⑤

E-Intelectual Property Theft - This ranges from stealing companies trade secrets, databases, digital music and videos, electronic documents and books, software and so on.

F-Brand Theft - It is quite easy to set up fake websites that look like real websites.

Eg: The attackers use the personal details provided by the innocent users to access the real site causing an identity theft.

② Publicity Attacks →

→ Publicity attacks occur because the attackers want to see their names appear on television news channels and newspapers.

→ These type of attackers are not hardware criminal.

→ They are the people such as students in universities or employees in large organizations, who seek publicity by adopting a novel approach of attacking computer systems.

→ They damages the web pages of a site by attacking it.

③ Legal Attacks →

→ The form of attack is novel and unique. The attacker tries to make the judge or the jury doubtful about the security of a computer system.

→ The attacker attacks the system and the attacked party manages to take the attacker to the court.

→ The aim of attacker is to exploit the weakness of the judge and the jury in technological matters

2) Technical View of Attack:

⇒ From a technical point of view, we can classify the types of attacks on computers and network systems into two categories for better understanding;

a) Theoretical Concepts
b) Pratical Approaches

a) Theoretical Concepts

⇒ The principles of security face threat from various attacks. These attacks are generally classified into four categories, & they are:

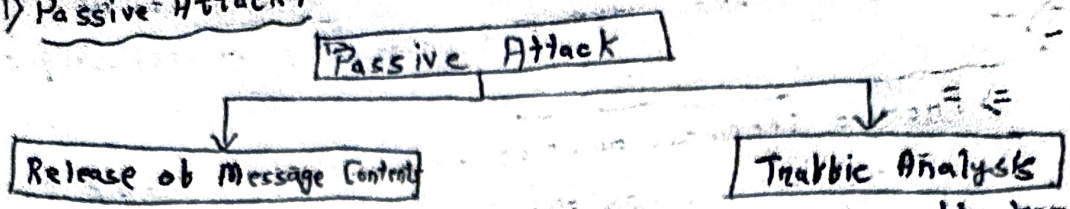
i) **Interception** – It is caused due to loss of message confidentiality which means an unauthorized party has gained access to a resource.
e.g. Copying of data or programs and listening to network traffic.

ii) **Fabrication** – It is caused due to the absence of proper authentication mechanisms.
eg. The attacker may add fake records to a database

iii) **Modification** – It is caused due to loss of message integrity. The attacker may modify/change/ temper the values in a database.

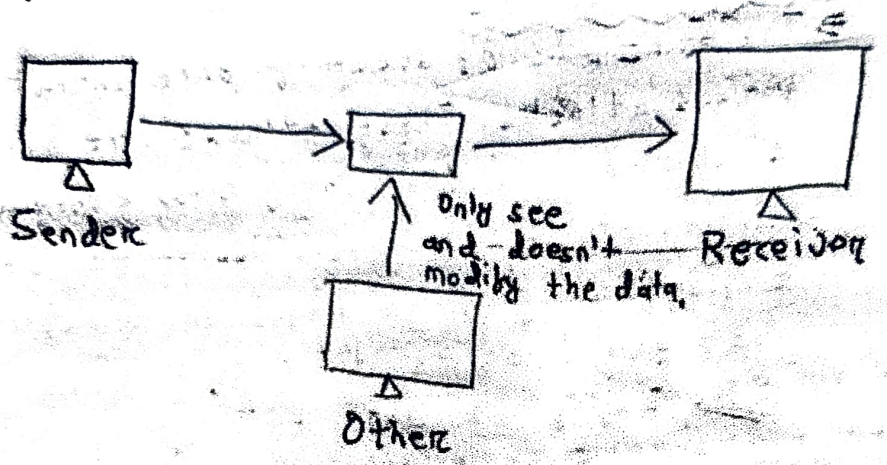
iv) **Interruption** – It is caused due to the context of availability of resources. The resource becomes unavailable, lost or unusable.
eg. Problems to hardware device, erasing program data or OS components.

1) Passive Attack:



→ Passive Attacks are those where in the attacker aims to obtain information that is in transit.

→ Passive attacks are harder to detect because the attacker dosen't modify the data.



→ The general approach to deal with passive attack is to think about prevention, rather than detection or corrective actions.

→ It doesn't involve any modifications to the contents of an original message.

→ These are two types of passive attacks;

i) Release of Message contents

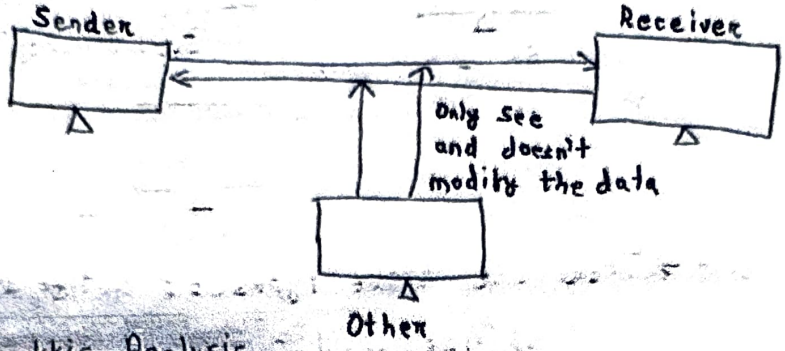
ii) Traffic Analysis

i) Release of Message Contents

→ Release of Message content is quite simple to understand when we send a confidential e-mail-message to our friend we desire that only third person able to access it.

Prepared by
Biswa Bandita Mohanty

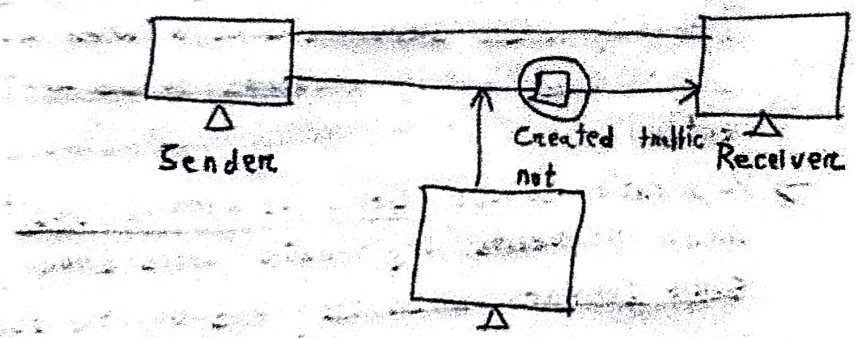
→ Using certain security mechanism, we can prevent 'the release of message contents',



ii) Traffic Analysis

→ It is the process of intercepting and examining message in order to deduce information from patterns in communication.

→ Attempts of analyzing (encoded) message to come up with likely patterns are the work of the 'traffic-analysis' attack.

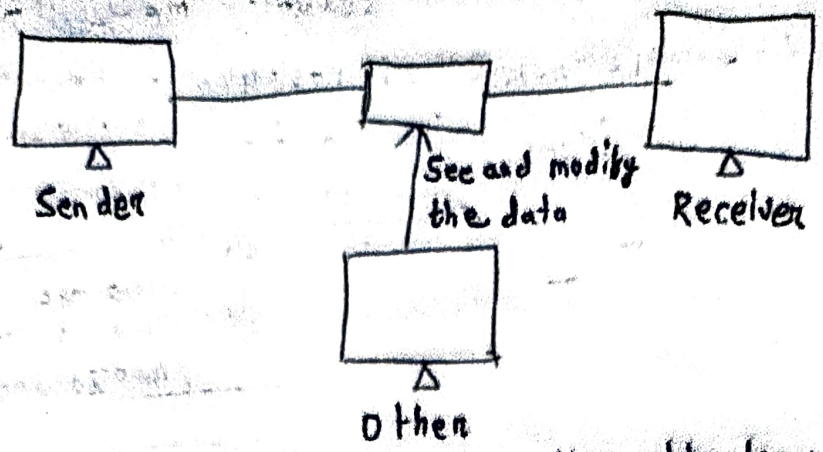


2) Active Attacks

→ It is based on the modification of the original message or in the creation of false message.

→ These attacks cannot be prevented easily.

→ These attacks can be in form of interruption, modification and fabrication.



→ There are three types of active attacks:

i) Masquerade
ii) Modification → Replay Attacks
→ Alterations
iii) Denial of Service (DOS)

→ Masquerade — An attacker creating a situation where the availability of a system is in danger, Same as 'Interception'.

→ Trying to pose as another entity involves 'masquerade' attacks, caused when an unauthorized entity pretends to be another entity.

→ Fabrication causes 'Denial of Service (DOS)' attacks, which prevents legitimate users from accessing some services, which they are eligible for.

→ In a replay attacks, a user captures a sequence of events or some data units and resends them.

→ In 'alteration of messages', it involves some change to the original message.

* Replay Attack → Attack on a system where in the attacker gets hold of a message and attempts to re-send it, hoping that the receiver doesn't detect this as a message sent twice.

Difference Between —

Passive Attack	Active Attack
→ Here, modification in the information doesn't take place	→ Here, modification in the information takes place.
→ It is danger for confidentiality	→ It is danger for integrity as well as availability
→ Here, attention is on prevention	→ Here, attention is on detection,
→ Due to passive attack, there is no harm to the system,	→ Due to active attacks, system is always damaged
→ Here, victim does not get informed about the attack	→ Here, victim gets informed about the attack.
→ System resources are not change	→ System resources can be changed.
→ Information and messages in the system or network are acquired,	→ Active attack influence the services of the system,
→ It is easy to prohibited then active attack,	→ It is tough to restrict from entering systems or networks

3) Pratical Side of Attacks

→ Security attacks can happen at the application level or network-level

① Application-Level Attacks →

→ These attacks happen at an application level in the sense that the attacker attempts to access, modify or prevent access to information of a particular application or to the application itself.

→ Example

Example of this earth trying to obtain someone's credit card information on the internet or changing the contents of a message to change the amount in transaction

Prepared by
Biswa Bandita Mohanty

② Network Level Attack

⇒ These attacks generally aim at reducing the capabilities of a network by a number of possible means.

⇒ These attacks either slowdown or completely bring to halt a computer network.

4) Program that Attack

⇒ A few programs that attack computer system to cause some damage or to create some confusion.

⇒ Program that attack –

i) Virus

→ A virus is a small computer program that attaches itself to another legimate program and cause damage to the computer system or to the network.

→ Virus can be classified into the following categories;

a) Parasitic Virus: The virus attaches itself to executable files and keep replicating. Whenever the file (infected file) is executed, the virus looks for other executable files to attach itself and spread.

b) Memory-resident Virus: The type of virus first attaches itself to an area of the main memory and then infects every executable program that is executed.

c) Boot sector Virus: The type of virus infects the master boot record of the disk and spreads on the disk when the operating system start booting the computer.

d) Stealth Virus: This virus has intelligence built-in, which prevents anti-virus software program from detecting it.

e) Polymorphic Virus: A virus that keeps changing its signature on every execution, making it very difficult to detect.

f) Metamorphic Virus: In addition to changing its signature like polymorphic virus, this type of virus keeps rewriting itself everytime making its detection even harder.

→ The phases of virus are as follows:

a) Dormant Phase → Here, the virus is idle. It gets activated based on a certain action or event. This is an optional phase.

b) Progation Phase → A virus copies itself and each copy starts creating more copies of itself

c) Triggering Phase → A dormat virus moves into this phase when the action/event for which it was waiting is initiated.

d) Execution Phase → This is the actual work of virus which could be harmless or destructive.

(ii) Worm

→ A worm is a small program doesn't perform any destructive actions but only consumes system resources to bring down the computer / network.

→ It doesn't modify a program.

→ It replicates itself by creating its own copies, mainly to bring the network to a halt.

Prepared by
Biswa Bandita Mohanty

(iii) Trojan Horse

→ A Trojan Horse allows an attacker to obtain some confidential information about a computer on a network.

5) Specific Attacks:

i) Sniffing → Sniffing attack or a sniffer attack in context of network security corresponds to theft or interception of data by capturing the network traffic using a sniffer tool.

ii) Spoofing → Spoofing is the process in which an intruder introduces fake traffic and pretends to be someone else.

iii) Phishing Attack → It is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

iv) Pharming (DNS Spoofing) → It is a form of cyber attack that sends the user to a fake website that looks like the real thing.